Yedla dinesh, Addanki purna ramesh / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 1, Jan-Feb 2012, pp.251-259

Efficient Capacity Image Steganography by Using Wavelets

Yedla dinesh Addanki purna ramesh

(Department of Electronics and communications, Sri vasavi engineering college, Tadepalligudem, AP, India)
(Department of Electronics and communications, Sri vasavi engineering college, Tadepalligudem, AP, India)

ABSTRACT
Data hiding techniques have taken important role with the rapid growth of intensive transfer of multimedia content and secret communications. Steganography is the art of hiding information in ways that prevent detection. The wavelet transform has gained widespread acceptance in image processing. Discrete Wavelet Transform performs a multi-resolution analysis and space frequency localization. The proposed Steganography algorithm works on the haar and daubechies wavelet transform coefficients of the original image to embed the secret image. Here discrete wavelet transforms is used to transform the both original image and secret image. So discrete wavelet transforms allows perfect embedding of the hidden message and reconstruction. As compared to the current transform domain data hiding methods [1] this scheme can provide an efficient capacity for data hiding without sacrificing the original image quality.

Keywords- **Discrete Wavelet transforms, Bit Plane Complexity segmentation, Capacity**

I. INTRODUCTION
With advancements in Digital Communication Technology Data hiding takes place as an important role. The redundancy of digital media, as well as the characteristic of the human visual system makes it possible to hide messages [10]. Steganography is one of the data hiding scheme which is the science that involves communicating secret data in an appropriate multimedia carrier. It can embed any image, audio and video files. Steganography's ultimate objectives which are undetectable, robustness resistance to various image processing methods and compression, and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. Our main goal in steganography is to provide more capacity and robustness.

Steganography techniques are mainly divided in to two categories. The method consists consist of embedding the secret file in the image domain or also called as the spatial domain. The other technique hides the secret file in the transform domain or frequency domain of an image. As compared to the spatial domain techniques in transform domain alterations are made in the frequency domain of the image and hiding the message in it by using a few transformations on the image. By using this technique the message is hidden in significant areas of the image making it more robust and difficult to trace. A few transforms used for these techniques are Integer wavelet transforms and Discrete Wavelet transforms. This is the main theme of the current paper.

The compatibility of the Human Visual System is the additional advantage in wavelet transforms. The methods mentioned by the image watermarking are having a limited capacity [8][9]. There are few steganography schemes developed by using wavelets. For example Hay-ying, L.Xu introduced an algorithm that concealed the message directly in jpeg2000 compressed bit stream [4]. But these methods have limited data embedding capacity. Compared to these techniques steganography using BPCS to the integer wavelet transformed image [7] has improvement in capacity.

In our proposed method we have used a new approach to embed the data in the images. This technique provides an efficient capacity in data hiding compared to the previous methods without sacrificing the original image quality.

1. Implementation

1.1 Discrete Wavelet transforms

The proposed scheme uses discrete wavelet transforms to presentation of the Original image to conceal the secret message. Here we have used the haar wavelets and daubechies wavelets of the image to conceal the secret message. Wavelet transform divides the information of an image in to approximation and detail sub signals. The LL band includes the low pass coefficients and represents a soft approximation to the image and other three detail sub signals shows the vertical, horizontal and diagonal details or changes in the images.

1.1.1 Haar wavelet transforms

To understand how wavelets work, let us start with a simple example. Assume we have a 1D image with a resolution of four pixels, having values [9 7 3 5]. Haar wavelet basis can be used to represent this image by computing a wavelet transform. To do this, first the average the pixels together, pair wise, is calculated to get the new lower resolution image with pixel values [8 4]. Clearly, some information is lost in this averaging process. We need to store some detail coefficients to recover the original four pixel values from the two averaged values. In our example, 1 is chosen for the first detail coefficient, since the average computed is 1 less than 9 and 1 more than 7. This single number is used to recover the first two pixels of our original four-pixel image. Similarly, the Second detail coefficient is -1, since 4 + (-1) = 3 and 4 - (-1) =5. Thus, the original image is decomposed into a lower resolution (two-pixel) version and a pair of detail coefficients. Repeating this process recursively on the averages gives the full decomposition shown in Table 1.

Table 1

Resolution	Averages	Detail Coefficients
4	[9 7 3 5]	
2	[8 4]	[1 -1]
1	[6]	[2]

Decomposition to lower resolution

Thus, for the one-dimensional Haar basis, the wavelet Transform of the original four-pixel image is given by [6 2 1 -1]. We call the way used to compute the wavelet transform by recursively averaging and differencing coefficients, filter bank. We can reconstruct the image to any resolution by recursively adding and subtracting the detail coefficients from the lower resolution versions.

The basic functions for the spaces (V^j) are called scaling functions and wavelet functions which are denoted by the symbol ϕ and ψ. A simple basis for V^j is given by the set of scaled and translated box functions

$$\Phi_{r,s}(x) = 2^{r/2}\phi(2^r x - s) \quad (1)$$

Where r, s is the integers and x is a variable in continuous space.

$$\Phi[x] = \begin{cases} 1, x \in [0,1) \\ 0, otherwise \end{cases}$$

And the wavelet functions are given by $\Psi_{r,s}$

$$\Psi_{r,s}(x) = 2^{r/2}\psi(2^r x - s) \quad (2)$$

$$\Psi[x] = \begin{cases} 1, 0 \le x \le 0.5 \\ -1, 0.5 \le x \le 1 \\ 0, elsewhere \end{cases}$$

Whatever function is there with in the first subspace even that also we should be able to analyze using the function which covers the next subspace and based on this subspace coverage arguments are given as

$$\Phi(x) = \sum_n h\phi(n)\sqrt{2}\phi(2x - n) \quad (3)$$

$$\Psi(x) = \sum_n h\psi(n)\sqrt{2}\phi(2x - n) \quad (4)$$

The DWT for an image as a 2D signal will be obtained from 1D DWT. We get the scaling function and wavelet function for 2D by multiplying two 1D functions. The scaling function is obtained by multiplying two 1D scaling functions: $\phi(x, y) = \phi(x)\,\phi(y)$. The wavelet functions are obtained by multiplying two wavelet functions or wavelet and scaling function for 1D. For 2D case there exist three wavelet functions that scan details in horizontal $\Psi^H(x,y) = \Psi(x)\,\phi(y)$, vertical $\Psi^V(x, y) = \phi(x)\,\Psi(y)$ and diagonal directions: $\Psi^{D} = \Psi(x)\,\Psi(y)$.

This may be represented as four channel perfect reconstruction filter bank as shown in Fig 1. Now each filter is 2D with the subscript indicating the type of filter (HPF or LPF) for separable horizontal and vertical components. By using these filters in one stage, an image is decomposed in to four bands. There exist three types of detail images for each resolution: horizontal (HL), vertical (LH) and diagonal (HH). The operations can be repeated on the low low (LL) band using the second stage of identical filter bank. The 2 level discrete wavelet transform is shown in Fig 2.

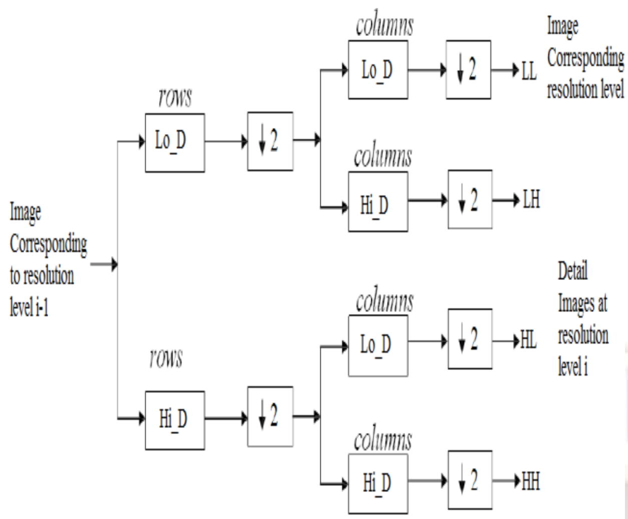


Figure 1.One Filter Stage in 2D DWT

Figure2. 2level discrete wavelet transform

In Haar basis the transform is given as X[2k]=$\frac{1}{\sqrt{2}}$(x[2k] + x[2k+1]), X[2k+1]= $\frac{1}{\sqrt{2}}$(x[2k]-x[2k-1]) and the reconstruction is obtained from x[n]=$\sum_{k\epsilon z} X[k]\phi_k[n]$. The Transformation of the 2D image is a 2D generalization of the 1D wavelet transform. It applies the 1D wavelet transform to each row of pixel values. This operation provides us an average value along with detail coefficients for each row. Next, the transformed are treated as if they were themselves an image and apply the 1D transform to each column. The resulting values are all detail coefficients except a single overall average coefficient. In order to complete the transformation, this process is repeated recursively only on the quadrant containing averages.

1.1.2 Daubechies wavelet transforms

Daubechies wavelets are a family of orthogonal wavelets defining a discrete wavelet transforms and characterized by a maximal number of vanishing moments for some given support. This kind of 2DDWT aims to decompose the image into approximation coefficients (cA) and detailed coefficient cH, cV and cD(horizontal, vertical and diagonal) obtained by wavelet decomposition of the Original image.

This is based on the four magic numbers h_0, h_1, h_2 and h_3. It has compact support and zero moments of father function

$$M_i = \int x\Phi(x)dx = 0 \qquad (5)$$

and from the below first two equations corresponding to the orthonormality in L_2, and third equation to satisfy dialation equation and fourth one refers to the moment of the father function.

$$h_0^2 + h_1^2 + h_2^2 + h_3^2 = 1 \qquad (6)$$

$$h_0h_2 + h_1h_3 = 0 \qquad (7)$$

$$h_0 + h_1 + h_2 + h_3 = \sqrt{2} \qquad (8)$$

$$h_1 + 2h_2 + 3h_3 = 0 \qquad (9)$$

Wavelet transforms are multi-resolution image decomposition tool that provide a variety of channels representing the image feature by different frequency sub bands at multi-scale. When decomposition is performed, the approximation and detail component can be separated. The steps for decomposition and reconstruction of an image are shown in the Fig3 and Fig4 below.

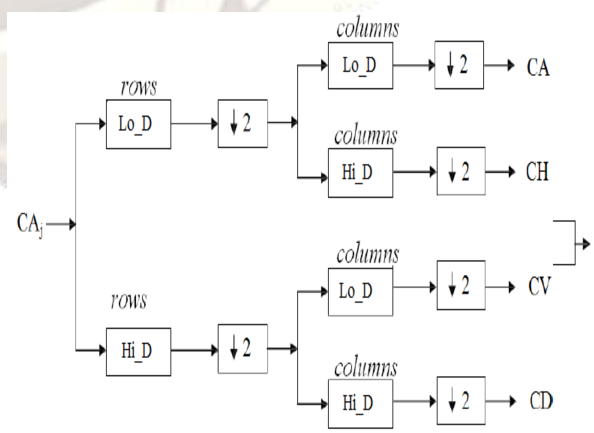


Figure 3. Steps for decomposition of an image

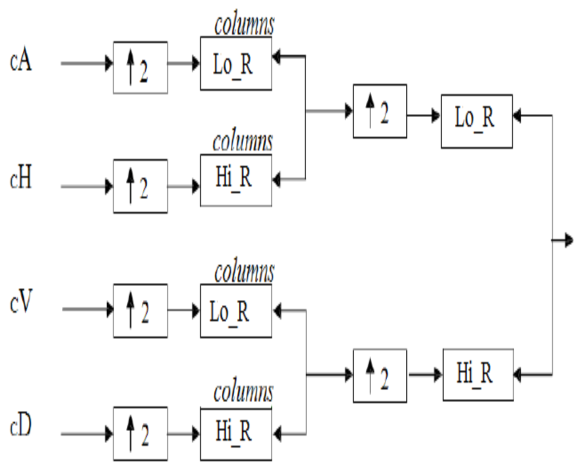


Figure 4. Steps for reconstruction of an image

In daubechies wavelet transforms, the wavelet type balanced frequency responses. These use overlapping windows, so the high frequency coefficients spectrum reflects all high frequency changes. Therefore these are useful in image processing and noise removal of audio signal processing.

2 Bit Plane Complexity Segmentation

The Original image is divided in to bit planes using bit plane decomposition technique, and from this the complexity is calculated to find the capacity of blocks and hidden source is embedded. Due to that in this the calculation is based on the image complexity on each bit plane. In this we used the black and white border complexity measurement for determining the complexity of a block.

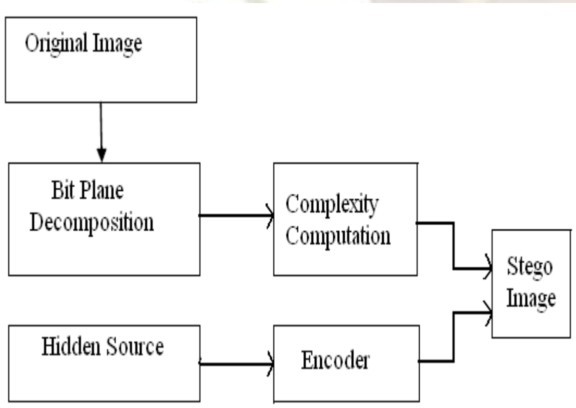


Figure 5. BPCS model for image steganography to obtain a stego image.

2.1 Block Segmentation

We take each bit corresponding to its position and form eight corresponding bit planes as we can see from the Fig 4 shown below [1]. We divide each sub blocks in to bit planes each of size 8×8. We need to check for the complexity of each of these sub blocks to determine the complexity and then capacity. We rearrange the secret data by determining the capacity of blocks and embed without affecting the original image.

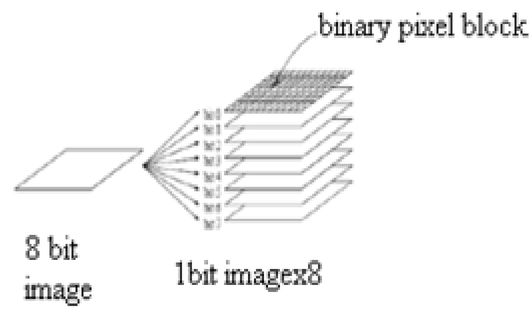


Figure 6. Decomposition into bit planes

The capacity of the blocks is determined by the maximum complexity in the relavant channel and comparative threshold used for making decision on the planes of that channel.

2.2 Complexity measurement

The complexity measure is given by

$$\alpha = \frac{k}{The\ Max\ Possible\ \ B{-}Wchanges\ \ in\ image} \qquad (10)$$

Where k is the total length of black and white border in that particular image leading to values of α such that $0 < \alpha < 1$. Consider for a case of square binary image consisting of 2^n rows and 2^n columns ($2^n \times 2^n$) the maximum number of black and white changes in the image would be given by $2 \times 2^n \times (2^n - 1)$. Then the complexity measure 'α' is defined as

$$\alpha = \frac{k}{2 \times 2^n \times (2^n - 1)}$$

Where $0 \leq k \leq 2 \times 2^n \times (2^n - 1)$

A simple example is if we consider a black pixel surrounded by four white pixels which are having all its four connected neighbors as white pixels, we will have a border length of four. This is because there are two color changes along the row and also along the column making a total of 4.

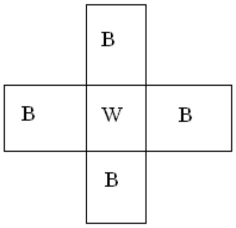


Figure 7.Single white pixel surrounded by four black pixels.

3 Algorithmic approaches

The block diagram of the embedding procedure is shown in Fig 8.

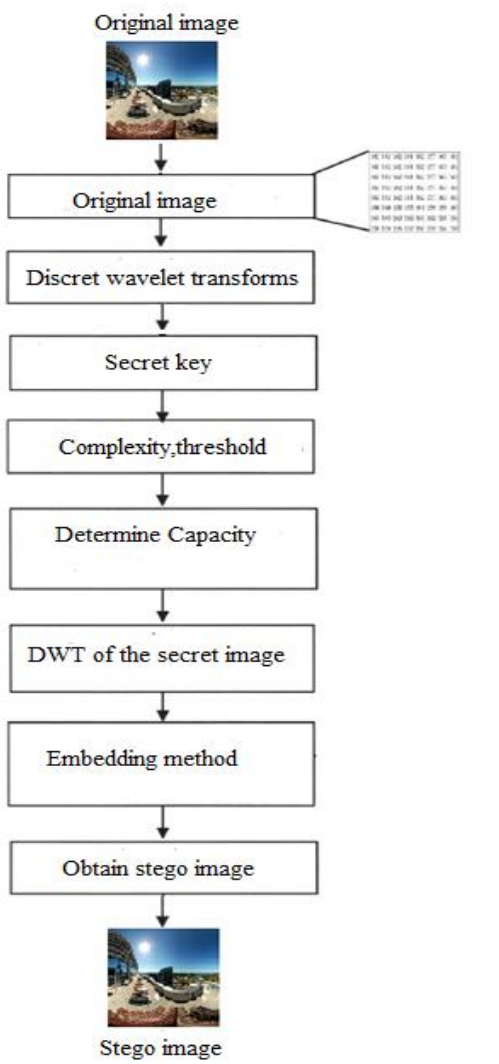


Figure 8. Block diagram of the embedding algorithm

The blocks of embedding algorithm is explained in the following steps

Step 1: Consider a Original image

Step 2: Apply 2level Discrete wavelet transforms for the original image and segment it into 8×8 blocks.

Step 3: The secret key is used to determine the order of blocks selected for embedding.

Step 4: The maximum complexity of blocks is calculated for each channel, and also threshold calculation.

$T=\frac{\alpha}{N}\sum^{N}|I_W|$

Where I_w's are the coefficients of discrete wavelet transforms for the original image, N is the number of coefficients.

Step 5: The Capacity of the each block is determined finding its first MSB plane possessing a complexity higher than the threshold.

Step 6: Apply the 2level discrete wavelet transforms for the secret image.

Step 7: The embedding method is described as, After transforming the original image A, let us consider the coefficients of size $G_A \times H_A$ represented as

$A=\{C_{ij}|0 \le i < G_A , 0 \le j < H_A\}$

Where C_{ij} are the coefficients corresponding to the RGB channels in the transformed image. and M be the DWT coefficients of the secret message 's'.

$M=\{m_{ij} |0 \le i < s, 0 \le j < s\}$

where m_{ij} belongs to the corresponding coefficients of the transformed secret image. For the embedding of the 's' coefficients of the secret message M into the capacity of the blocks in the transformed image we first rearrange the secret message M* as

$M^*=\{m^*_{ij}|0 \le i < s^*, 0 \le j < s^*, m^*_{ij} \{0,1,...,2^c-1\}\}$

Where c is the total capacity of blocks and $s^* < G_A \times H_A$, then we form the coefficients by

$M^*_{ij}= \sum_{k=0}^{c-1} m_{ij\times c+k} \times 2^{c-1-k}$

In the transformed image, if the value of the DWT coefficient is less than the threshold, then embedding process is done by storing the secret message coefficients m^*_{ij} to C_{ij}. So the set of coefficients $\{C_1,C_2,......Cs^*\}$ of C_{ij} of the chosen coefficients for storing secret message coefficients m^*_{ij} is modified to form the stego image coefficients C^*_{ij} as follows

$C^*_{ij} = C_{ij} - C_{ij} \bmod 2^c + m^*_{ij}$

Step 8: Finally the stego image is formed.

The block diagram of extracting procedure is shown in Fig 9

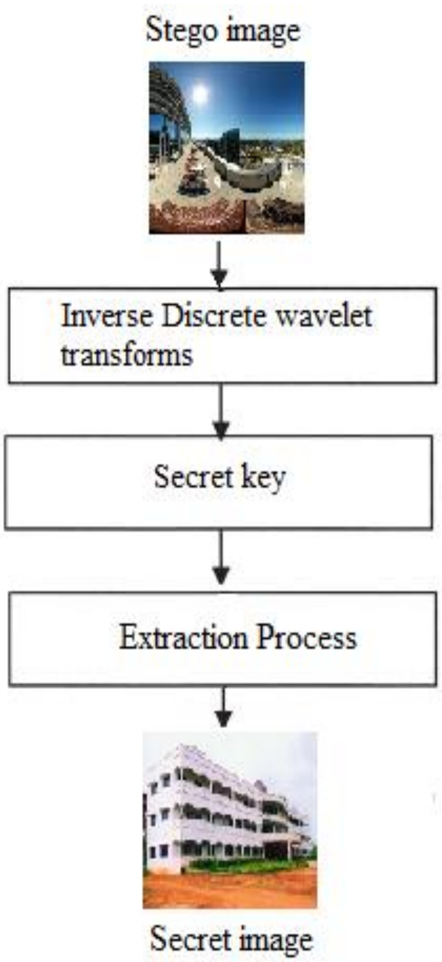


Figure 9: Block diagram of the Extracting algorithm.

The blocks of Extracting algorithm is explained in the following steps.

Step 1: Apply inverse 2level discrete wavelet transforms to the original image and secret image.

Step 2: The secret key is used for extracting the secret images.

Step 3: In Extraction process the secret images are extracted. The set of coefficients $\{C^*_1, C^*_2, ...C^*s^*\}$ storing the secret message coefficients are selected and reconstructed. So the embedded secret message coefficients m_{ij} can be recovered by $m_{ij} = C^*_{ij} \bmod 2^c$.

III. RESULTS

The 512×512 original image is considered in our experiments and compared to the performance of our method to that of the previous method [1]. Here we have used discrete wavelet transforms and Bit plane complexity segmentation to hide the secret images. Therefore we can compare the capacity and the image quality obtained using the same threshold in both methods. In our experiment we have shown the normalized results for haar and daubechies wavelet transforms and obtained the results compared to the previous method with new approach for jpeg images. This is also applicable to other types of discrete wavelets. This shows that we have an efficient capacity. Usually the invisibility of the hidden messages is measured in terms of Peak Signal to Noise Ratio.

$$PSNR = 10 \log_{10}(S^2/MSE) \qquad (11)$$

Where

$$S^2 = \frac{1}{M \times N} \sum_{i=1}^{m} \sum_{j=1}^{n} J^2\,(i,j) \qquad (12)$$

And Mean Square error is defined as

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{m} \sum_{j=1}^{n} [J(i,j) - J^{'}(i,j)]^2 \quad (13)$$

Where J represents the coefficients in stego image.

Encryption of secret image by using haar wavelets in original image

Figure 10. Original Image

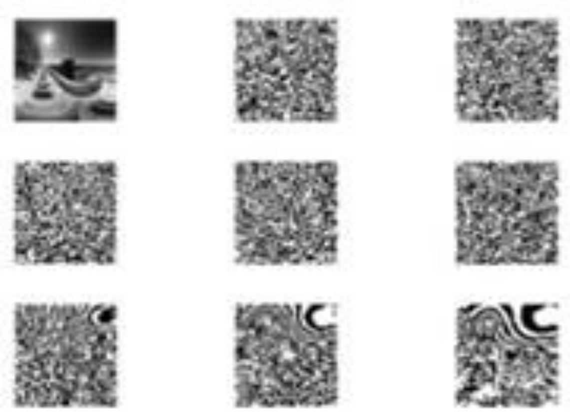


Figure 11. BPCS Image

Figure 12.Secret Image

Figure 13 Stego Image

Decryption of secret image by using haar wavelets

Figure 14.Extracted Secret Image

Table II

Threshold		Applied method	Previous method
0.3	BPP	15.5	15.1
	PSNR	19.1	18.4
0.4	BPP	14.9	14.4
	PSNR	20.1	19.6
0.5	BPP	13.8	13.5
	PSNR	22.3	21.6
0.6	BPP	12.9	12.3
	PSNR	25.2	24.3

Results by using haar wavelets with secret image embedded in original image. (normalized results)

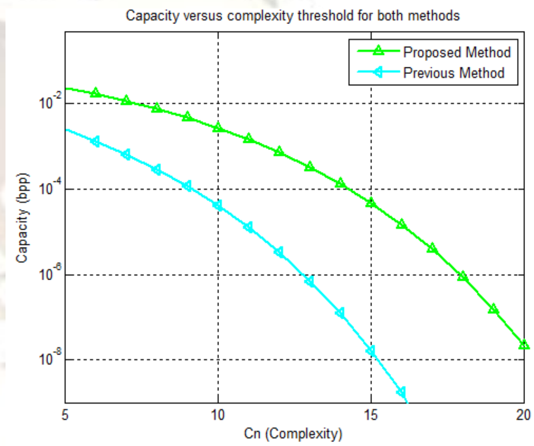


Figure 15.Capacity versus complexity threshold for both methods.

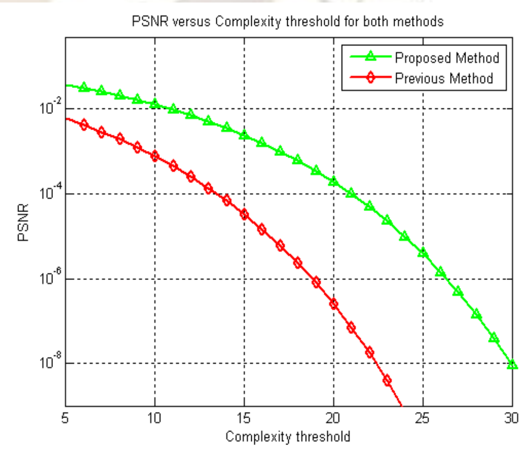


Figure 16. PSNR versus complexity threshold for both methods.

Encryption of secret image by using Daubechies wavelets in original image

Figure 17. Original Image

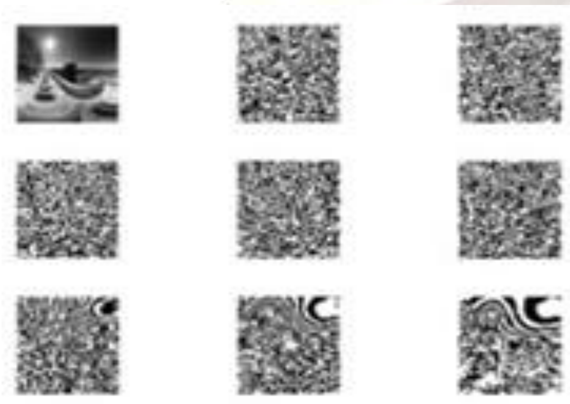


Figure 18. BPCS Image

Figure 19.Secret Image

Figure 20. Stego Image

Decryption of secret image by using Daubechies wavelets

Figure 21.Extracted Secret Image

Table III

Threshold		Applied method	Previous method
0.3	BPP	16.2	15.1
	PSNR	20.1	18.4
0.4	BPP	15.6	14.4
	PSNR	21.1	19.6
0.5	BPP	14.8	13.5
	PSNR	22.8	21.6
0.6	BPP	13.2	12.3
	PSNR	26.3	24.3

Results by using daubechies wavelets with secret image embedded in original image (normalized results)

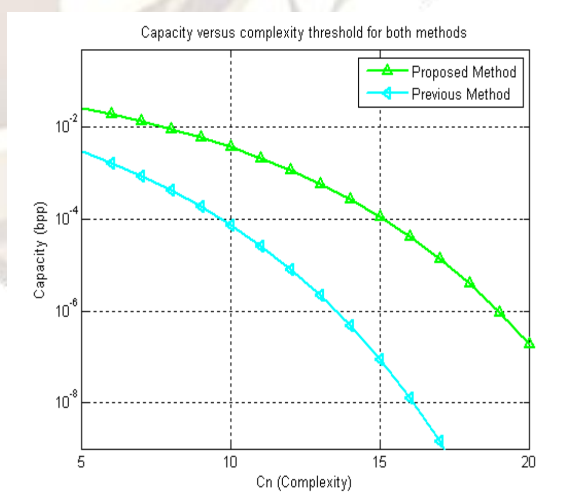
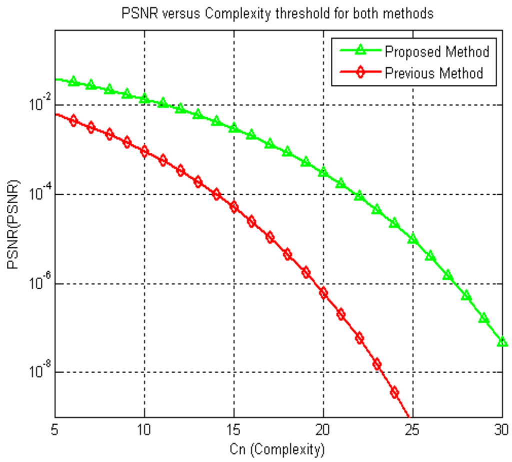


Figure 15.Capacity versus complexity threshold for both methods



.Figure 16. PSNR versus complexity threshold for both methods.

IV. CONCLUSION

This method pre-adjusts the original image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value to recover the secret message correctly. The discrete wavelet transform provided satisfactory results for image steganography application. The results also indicate a significant improvement in capacity and quality of the stego image when compared to the previous method. Wavelet transform allows perfect embedding of the hidden message and reconstruction. Therefore, there is a significant improvement in capacity as compared to that offered by previous methods, as confirmed by our experiments. We have designed an efficient capacity image steganography by using discrete wavelet transforms and bit plane complexity segmentation.

REFERENCES

[1] S.sarreshtedari,S.Ghaemmaghami"HighCapacity Image Steganography in Wavelet Domain" IEEE 2010.
[2] Srikanth.S.Khaire,Sanjay.L.Nalbalwar"Steganography- Bit Plane Complexity Segmentatiion Technique in International Science of engineering science and technology, 2010.
[3] S.sarreshtedari,M.Ghotbi,S.Ghaemmaghami,"One-third probability embedding:less detectable steganography," july 2009.
[4] G. Hay-ying, X.Yin, L.Xu and L.Guo-qiang, "A Steganographic algorithm for JPEG2000 in *Conference on computer science and software engineering, 2008.*
[5] S.E.El-Khamy, M.Khedr, A.Alkabbany "A hybrid fractal-wavelet data hiding technique" 25th NRCS, March 2008.
[6] N.Bi.Q.sun, D.Huang, Z.yang and j.Huang,"Robust Watermarking based on multiband wavelets and empirical Mode decomposition," *IEEE transaction on image processing 2007.*
[7] M.K.Ramani, E.V.Prasad, S.Varadarajan, "Steganography using BPCS to the integer wavelet transformed image" IJCSNS 2007.
[8] T.G.Gao ,Q.L.Gu, "Reversible watermarking algorithm based on wavelet lifting scheme," Wavelet analysis and pattern recognition conference, November 2007.
[9] L.Sunil, C.D.YooT.Kalker, "Reversible Image Watermarking based on Integer-to-Integer Wavelet Transform", IEEE Transaction of information, forensics and security, September 2007.
[10] D.Artz, "Digital steganography: hiding data within data," IEEE Internet Computing, pp.75-80, May-June 2001.